



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/611,460	06/30/2003	Tzong-Fen Fuh	50325-0799	1623
29989 7590 04/10/2007 HICKMAN PALERMO TRUONG & BECKER, LLP 2055 GATEWAY PLACE SUITE 550 SAN JOSE, CA 95110			EXAMINER WHIPPLE, BRIAN P	
			ART UNIT 2152	PAPER NUMBER

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/10/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/611,460	FUH ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Brian P. Whipple	2152	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 30 June 2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>12/05/2003</u>  | 6) <input type="checkbox"/> Other: _____                          |

### DETAILED ACTION

1. Claims 1-30 are pending in this application and presented for examination.

#### ***Double Patenting***

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1-7, 9-10, 13, 15-17, and 19 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 18 of U.S. Patent No. 6,609,154 B1 ('154). Although the conflicting claims are not identical, they are not patentably distinct from each other because creating and storing authorization information comprises creating and storing authorization information for each client in a cache and authenticating login information is accomplished by using a profile stored in an authentication server.

4. Claims 1-7, 9-10, 13, 15-17, and 19 correspond to claim 18 of '154.

***Claim Rejections - 35 USC § 112***

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. As to claims 1 and 15, the claims are rejected for lack of antecedent basis. In claim 1, ln. 4-5 and Claim 15, ln. 3-4, the phrase "the network firewall routing device" lacks antecedent basis.

8. As to claim 2, it is unclear how client authorization information can comprise means in a network firewall routing device for caching client authorization information. Client authorization information would appear to be logical, so it is unclear how information could comprise means for storing information in a physical device. Additionally, it is unclear how the client authorization information could store said client authorization information, as this appears to be a circular definition of said information.

The examiner interpreted "wherein the client authorization information comprises" as wherein the means for creating and storing client authorization information comprises.

9. As to claims 3-4, it is unclear if authentication cache refers to physical caches or a plurality of logical cache entries. The instant specification leads to the conclusion that the caches are logical entities, as it is stated, "the firewall router 210 also includes any number of authentication caches... Each authentication cache represents a valid user authentication" ([0063]). The examiner interpreted the authentication caches as logical entities for the purposes of examination.

10. Additionally, claim 4 is indefinite, as it is unclear how client authorization information can comprise a plurality of authentication caches, each cache associated with a unique client. Client authorization information comprising a plurality of caches each containing an entry of authorization information for a client appears to be a circular definition. The examiner interpreted "wherein the client authorization information comprises" as wherein the means for creating and storing client authorization information comprises.

11. As to claim 12, "the updated authentication information" and "each authentication cache" lack antecedent basis.

12. As to claim 16, the claim is rejected for the same reasons as claim 4 above.

13. As to claim 18, the claim is rejected for lack of antecedent basis. In claim 18, ln. 5, "the source IP address" lacks antecedent basis.

***Claim Rejections - 35 USC § 102***

14. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

15. Claims 1, 5-9, 14-15, 17-18, 22-23, and 25-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Baize, U.S. Patent No. 6,317,838 B1.

16. As to claim 1, Baize discloses a system for controlling access of a client to a network resource (Abstract, ln. 1-3), the system comprising:

a network resource that is communicatively coupled to a network (Fig. 1; Col. 5, ln. 13-22);

an authentication server that is communicatively coupled to the network and to the network firewall routing device and comprising user profile information (Fig. 1, **Security Server SS**; Abstract, ln. 5-11);

a network firewall routing device that is communicatively coupled to the network and that is logically interposed between the client and the network resource (Fig. 1; Abstract, ln. 1-3; Col. 6, ln. 3-9);

means for creating and storing client authorization information at the network firewall routing device, based in part on the user profile information, wherein the client authorization information comprises information indicating whether the client is authorized to communicate with the network resource and information indicating what access privileges the client has with respect to the network resource (Col. 6, ln. 58 – Col. 7, ln. 14; Col. 8, ln. 4-6);

means for receiving a request from the client to communicate with the network resource (Col. 4, ln. 38-42);

means for determining whether the client is authorized to communicate with the network resource based on the authorization information (Col. 4, ln. 43-48); and

means for reconfiguring the network firewall routing device to permit the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on the authorization information (Col. 6, ln. 33-42; Col. 7, ln. 15-18).

17. As to claim 5, Baize discloses means for determining whether the client is authorized to communicate with the network resource comprises means for matching information in the request identifying the client to information in means for filtering in the

Art Unit: 2152

network routing device and to the authorization information stored in the network firewall routing device (Col. 4, ln. 38-48).

18. As to claim 6, Baize discloses means for determining whether the client is authorized to communicate with the network resource comprises: means for matching a source IP address of the client in a data packet of the request to information in a filtering mechanism of the network routing device (Col. 2, ln. 55-59; Col. 6, ln. 14-21, 33-42, and 62-65); and

means for matching the source IP address to the authorization information stored in the network firewall routing device if the source IP address matches the information in the filtering mechanism of the network routing device (Col. 6, ln. 66 – Col. 7, ln. 14).

19. As to claim 7, Baize discloses means for determining whether the client is authorized to communicate with the network resource comprises: means for matching a source IP address of the client in a data packet of the request to information in a means for filtering in the network routing device (Col. 2, ln. 55-59; Col. 6, ln. 14-21, 33-42, and 62-65);

means for matching the source IP address to the authorization information stored in the network firewall routing device if the source IP address matches the information in the filtering mechanism of the network routing device (Col. 6, ln. 66 – Col. 7, ln. 14); and



means for matching user identifying information received from the client to a profile associated with the user that is stored in the authentication server if the source IP address fails to match the authorization information stored in the network firewall routing device (Col. 6, ln. 62 – Col. 7, ln. 18).

20. As to claim 8, Baize discloses means for determining whether the client is authorized to communicate with the network resource comprises: means for matching a source IP address of the client in a data packet of the request to information in a filtering mechanism of the network routing device (Col. 2, ln. 55-59; Col. 6, ln. 14-21, 33-42, and 62-65);

means for matching the source IP address to the authorization information stored in the network firewall routing device if the source IP address matches the information in the filtering mechanism of the network routing device (Col. 6, ln. 66 – Col. 7, ln. 14); and

means for matching user identifying information received from the client to a profile associated with the user that is stored in a database server and is retrieved from the database server by the authentication server, if the source IP address fails to match the authorization information stored in the network firewall routing device (Fig. 1, **Data Base DBS** and **Security Server SS**; Col. 5, ln. 28-31; Col. 6, ln. 62 – Col. 7, ln. 18).

21. As to claim 9, Baize discloses means for determining whether the client is authorized to communicate with the network resource comprises: means for matching

client identifying information in the request to information in a filtering mechanism of the network routing device (Col. 2, In. 55-59; Col. 6, In. 14-21, 33-42, and 62-65);

means for matching the client identifying information to the authorization information stored in the network firewall routing device, if a match is found using the filtering mechanism (Col. 6, In. 66 – Col. 7, In. 14); and

means used, only when the client identifying information fails to match the authorization information stored in the network firewall routing device, for: creating and storing new authorization information in the network firewall routing device that is uniquely associated with the client (Col. 6, In. 58 – Col. 7, In. 14; Col. 8, In. 4-6);

requesting login information from the client (Col. 6, In. 62-65);

authenticating the login information by communicating with the authentication server (Col. 6, In. 62 – Col. 7, In. 2); and

updating the new authorization information based on information received from the authentication server (Col. 6, In. 66 – Col. 7, In. 14).

22. As to claim 14, Baize discloses means for reconfiguring the network firewall routing device comprises means for creating and storing one or more commands to the network firewall routing device which, when executed by the network firewall routing device, result in modifying one or more routing interfaces of the network firewall routing device to permit communication between the client and the network resource (Col. 6, In. 62 – Col. 7, In. 18).

23. As to claim 15, the claim is rejected for the same reasons as claim 1 above.

24. As to claim 17, the claim is rejected for the same reasons as claim 6 above.

25. As to claim 18, the claim is rejected for the same reasons as claim 8 above.

26. As to claim 22, Baize discloses a system for authentication comprising: a network resource connected to a network (Fig. 1; Col. 5, ln. 13-22);

a client capable of sending a request to communicate with the network resource (Col. 4, ln. 38-42);

a network firewall routing device that is logically interposed between the client and the network resource and that permits the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on client authorization information stored in the network firewall routing device, wherein the client authorization information comprises information indicating whether the client is authorized to communicate with the network resource and information indicating what access privileges the client has with respect to the network resource (Col. 6, ln. 58 – Col. 7, ln. 14; Col. 8, ln. 4-6);

a database server that stores a plurality of user profiles, each user profile uniquely associated with one of a plurality of users that can use the client to send requests to communicate with the network resource (Col. 5, ln. 28-31);

an authentication server that is logically interposed between the network firewall routing device and the database server, and that is capable of communicating with the database server and retrieving from the database server a user profile (Fig. 1, **Data Base DBS and Security Server SS**; Col. 5, ln. 28-31; Col. 6, ln. 62 – Col. 7, ln. 18).

27. As to claim 23, Baize discloses the network resource comprises a target server capable of servicing a request sent under at least one of HyperText Transfer Protocol; File Transfer Protocol (Col. 6, ln. 33-36); and Internet Control Message Protocol.

28. As to claim 25, Baize discloses the network firewall routing device comprises: one or more processors (Fig. 2; Col. 6, ln. 13-26; it is inherent that a firewall executing access decisions contains one or more processors); and

a storage medium carrying one or more sequences of one or more instructions including instructions which, when executed by the one or more processors (Fig. 2; Col. 6, ln. 13-26; Col. 7, ln. 3-14; it is inherent that a firewall storing an operational profile has a storage medium), cause the one or more processors to perform the steps of:

creating and storing the client authorization information at the network firewall routing device (Col. 6, ln. 66 – Col. 7, ln. 18);

receiving the request from the client to communicate with the network resource (Col. 6, ln. 58-61);

determining whether the client is authorized to communicate with the network resource based on the client authorization information (Col. 6, ln. 62 – Col. 7, ln. 18); and

permitting the client to communicate with the network resource only when the client is authorized to communicate with the network resource based on the client authorization information (Col. 6, ln. 62 – Col. 7, ln. 18).

29. As to claim 26, the claim is rejected for the same reasons as claim 14 above.

30. As to claim 27, Baize discloses determining whether the client is authorized to communicate with the network resource comprises the steps of: determining whether client identifying information in the request matches information in a filtering mechanism of the network firewall routing device (Col. 6, ln. 58-65);

if a match is found using the filtering mechanism, determining whether the client identifying information matches the client authorization information stored in the network firewall routing device (Col. 6, ln. 66 – Col. 7, ln. 18); and

only when the client identifying information fails to match the client authorization information stored in the network firewall routing device (Col. 6, ln. 66 – Col. 7, ln. 18), then:

creating and storing new client authorization information in the network firewall routing device that is uniquely associated with the client (Col. 6, ln. 66 – Col. 7, ln. 18);

requesting login information from the client (Col. 6, ln. 62-65);

authenticating the login information by communicating with the authentication server (Col. 6, ln. 66 – Col. 7, ln. 18); and

updating the new client authorization information based on information received from the authentication server (Col. 6, ln. 66 – Col. 7, ln. 18).

***Claim Rejections - 35 USC § 103***

31. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

32. Claims 2-4, 12-13, 16, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baize as applied to claims 1, 9, and 15 above, in view of Coss et al. (Coss), U.S. Patent No. 6,170,012 B1.

33. As to claim 2, Baize discloses the invention substantially as in parent claim 1, but is silent on caching client authorization information for each client that communicates with the network firewall routing device.

However, Coss does disclose caching client authorization information for each client that communicates with the network firewall routing device (Col. 2, ln. 5-28).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Baize by caching client authorization information as

Art Unit: 2152

taught by Coss in order to avoid the need to apply a rule set to each incoming packet, which improves the performance of the firewall routing device (Coss, Col. 2, In. 5-18).

34. As to claim 3, the claim is rejected for the same reasons as claim 2 above.

35. As to claim 4, Baize discloses the invention substantially as in parent claim 1, but is silent on a plurality of authentication caches, each authentication cache uniquely associated with one of a plurality of clients that communicate with the network routing device, each authentication cache comprising information indicating whether the client is authorized to communicate with the network resource and information indicating what access privileges the client is authorized to have with respect to the network resource.

However, Coss does disclose a plurality of authentication caches (Col. 5, In. 36-53), each authentication cache uniquely associated with one of a plurality of clients that communicate with the network routing device (Col. 5, In. 43-48), each authentication cache comprising information indicating whether the client is authorized to communicate with the network resource and information indicating what access privileges the client is authorized to have with respect to the network resource (Fig. 3; Col. 4, In. 8-11 and 25-29).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Baize by using a plurality of authentication caches comprising information indicating whether each client is authorized to communicate with a network resource and under what access privileges as taught by Coss in order to

avoid the need to apply a rule set to each incoming packet, which improves the performance of the firewall routing device (Coss, Col. 2, ln. 5-18) and in order to safeguard against unauthorized access (Coss, Col. 1, ln. 12-16).

36. As to claim 12, Baize discloses the invention substantially as in parent claim 9, but is silent on means for creating and storing an inactivity timer for each authentication cache, wherein the inactivity timer expires when no communications are directed from the client to the network resource through the network firewall routing device during a pre-determined period of time, and means for removing the updated authentication information when the inactivity timer expires.

However, Coss does disclose means for creating and storing an inactivity timer for each authentication cache, wherein the inactivity timer expires when no communications are directed from the client to the network resource through the network firewall routing device during a pre-determined period of time, and means for removing the updated authentication information when the inactivity timer expires (Col. 4, ln. 45-46).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Baize by utilizing an inactivity timer to remove cache entries as taught by Coss in order to free up space in a cache and in order to improve security by requiring an inactive client to re-authenticate.



Art Unit: 2152

37. As to claims 13 and 19, the claims are rejected for the same reasons as claims 4 and 8 above.

38. As to claim 16, the claim is rejected for the same reasons as claim 4 above.

39. Claims 10-11, 21, 24, and 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baize as applied to claims 9, 15, 22, and 27 above, in view of Klassen, U.S. Patent No. 6,216,121 B1.

40. As to claim 10, Baize discloses the invention substantially as in parent claim 9, including means for the network firewall routing device requesting login information from the client to solicit a username and a user password (Col. 6, ln. 62-65) and means for authenticating the login information comprises means for determining, from a profile associated with a user of the client stored in the authentication server, whether the username and password are valid (Col. 6, ln. 66 – Col. 7, ln. 2), but is silent on sending a Hypertext Markup language login form to the client.

However, Klassen does disclose sending a Hypertext Markup language login form to the client (Fig. 5; Col. 5, ln. 3-5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Baize by using a Hypertext Markup language login form as taught by Klassen in order to make use of a standard means for a client to login to a system and in order to authenticate the identify of the client.

41. As to claim 11, the claim is rejected for the same reasons as claims 8 and 10 above.

42. As to claim 21, Baize discloses the invention substantially as in parent claim 15, but is silent on the client in a computer system executing a Web browser.

However, Klassen discloses the client in a computer system executing a Web browser (Fig. 5; Col. 5, ln. 3-5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Baize by using a Web browser as taught by Klassen in order to make use of a standard means for a client to communicate with the Internet.

43. As to claim 24, the claim is rejected for the same reasons as claim 21 above.

44. As to claims 28-29, the claims are rejected for the same reasons as claim 11 above.

45. As to claim 30, the claim is rejected for the same reasons as claim 10 above.

46. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Baize and Coss as applied to claim 19 above, and further in view of Klassen.

47. As to claim 20, the claim is rejected for the same reasons as claim 11 above.

### ***Conclusion***

48. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Coley et al., U.S. Patent No. 5,826,014 discloses a firewall system for protecting network elements connected to a public network.

Belville et al., U.S. Patent No. 5,828,833 discloses a method and system for allowing remote procedure calls through a network firewall.

Jade et al., U.S. Patent No. 5,944,823 discloses outside access to computer resources through a firewall.

Tanno, U.S. Patent No. 5,960,177 discloses a system for performing remote operation between firewall-equipped networks or devices.

Antur et al., U.S. Patent No. 6,212,558 B1 discloses a method and apparatus for configuring and managing firewalls and security devices.

Antur et al., U.S. Patent No. 6,243,815 B1 discloses a method and apparatus for reconfiguring and managing firewalls and security devices.

Digiacomio et al., U.S. Patent No. 6,301,667 B1 discloses a method and system for secure network management or high-speed Internet access CPE.

Clark et al., U.S. Patent No. 6,442,588 B1 discloses a method of administering a dynamic filtering firewall.

Nakazawa, U.S. Patent No. 6,643,778 B1 discloses a network system using a firewall dynamic control method.


49. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian P. Whipple whose telephone number is (571) 270-1244. The examiner can normally be reached on Mon-Fri (8:30 AM to 5:00 PM EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on (571) 272-3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BPW

Brian P. Whipple  
4/1/07



BUNJOB JAROENCHONWANIT  
SUPERVISORY PATENT EXAMINER